successful (Step 152), SmartDial is complete (Step 153). If authentication is not successful, SmartDial terminates (154).

[0059] Figure 9 provides a more detailed explanation of the authentication of the dial-in user referred to as Step 151 in Figure 8. A dial-up client (120) sends version information and a distinguished name (DN) of a dial-up client user to a PKI-Bridge (124) via the RAS (110) (Step 155). The PKI-Bridge (124) checks the version information and forwards the DN to the server-side cryptographic function (130) (Step 156). The server-side cryptographic function (130) generates a challenge string and forwards it to the PKI-Bridge (124) (Step 157). An example of the challenge string is described in detail below.

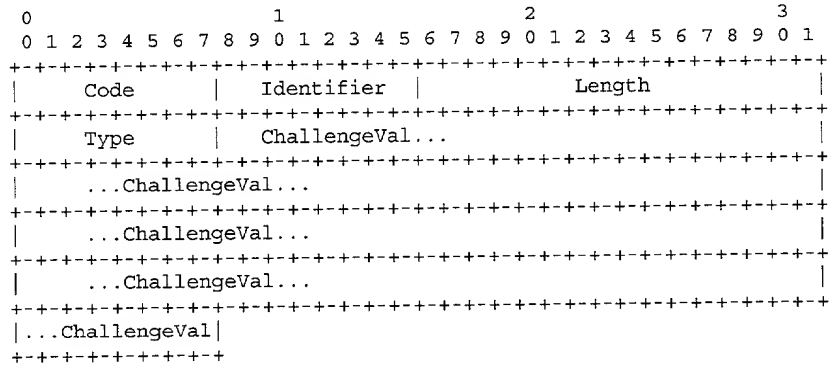
[0060] Next, the PKI-Bridge (124) forwards the challenge string to the dial-up client (120) (Step 158). The dial-up client (120) forwards the challenge string to the Custom Script DLL (122) (Step 159). The Custom Script DLL (122) forwards the challenge string to the client-side cryptographic function (128) (Step 160). The client-side cryptographic function (128) obtains the dial-up user's private key from a security device, and generates a signed response string (Step 161). An example of the signed response string is described in detail below.

[0061] Next, the client-side cryptographic function (128) forwards the signed response string to the Custom Script DLL (122) (Step 162). The Custom Script DLL (122) encodes the signed response string and divides the encoded signed response string into packets (Step 163). The Custom Script DLL (122) forwards the packets to the PKI-Bridge via dial-up client (120) and RAS (110) (Step 164).

[0062] The PKI-Bridge (124) receives the packets, reconstructs the encoded signed response string, and decodes the encoded response string (Step 165). The PKI-Bridge (124) forwards the reconstructed signed response string to the server-side cryptographic function (130) (Step 166). The server-side cryptographic function (130) obtains the user's public key from a directory server (114) using the DN

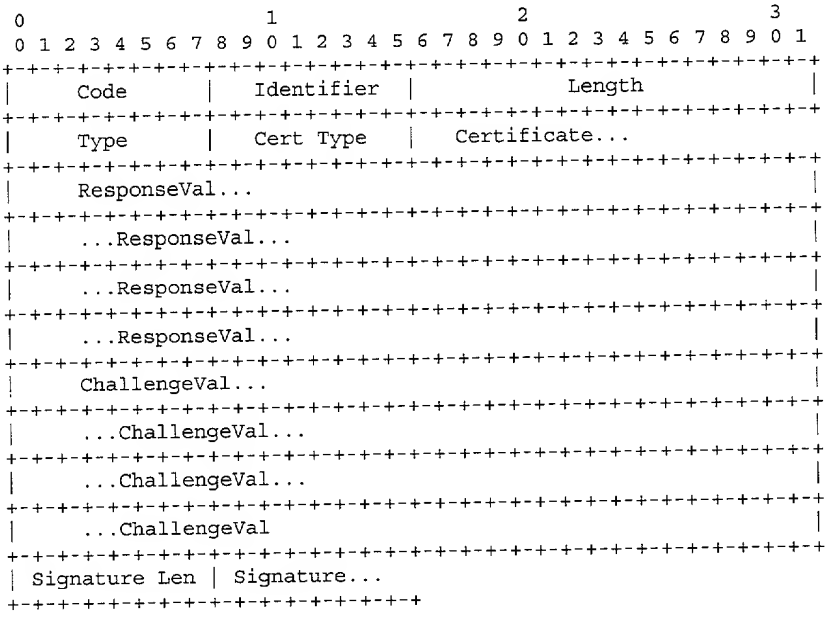
provided by the dial-up user (Step 167). The server-side cryptographic function (130) then verifies the reconstructed signed response string (Step 168).

[0063] In accordance with one or more embodiments, the client computer (102) responds to a challenge from the server-side cryptographic function (130) when connecting via SmartDial. The server-side cryptographic function (130) generates a random challenge for the client computer (102). To ensure that this challenge is not easily predictable, it is based on three factors: last sent challenge, current server time, and a randomly generated number. The entire challenge string is 16 octets in length. A summary of an authentication packet sent by the server (112) is shown below.



[0064] For the purposes of the summary of the authentication packet, a Code field value is 1. An Identifier field is one octet and aids in matching responses with requests. The Identifier field is changed on each request packet containing a different identifier. A Length field value is 21. The Type field value is to be determined by the Internet Assigned Numbers Authority (IANA). IANA is an organization that assigns protocol identification numbers. A ChallengeVal field is 16 octets of data, which is generated in a way to not be predictable by anyone. The ChallengeVal is sent only once, including those cases where no reply is given and the server re-transmits a challenge authentication packet.

[0065] In accordance with one or more embodiments, the client computer (102) uses the server-side cryptographic function (130) to perform normal certificate retrieval and signing functions when replying to the challenge. An example of a correct response to the challenge authentication packet from the server (112) is shown below.



[0066] For the purposes of the correct response to the challenge authentication packet from the server (112), the Code field is 2. The identifier field is one octet and matches the Identifier field from the corresponding request. The Length field is a two octet field and indicates the length of the authentication reply packet including the Code, Identifier, Length, Type, Certificate, Random Data, Echo Value, Signature Length, and Signature fields. The Type field value is to be determined by the IAAN. A Certificate Type field identifies the type of certificate the dial-up client (120) is presenting. In this implementation, the Certificate Type field is set to 1 to represent a X.509 certificate. The Certificate field is the dial-up client's (120) X.509 certificate from the server-side cryptographic function (130). The ResponseVal field is a sixteen-octet field. The field is generated by the dial-